

CLAIMS:

1. A method for protecting packets to be sent from a first network node to a second network node, comprising the steps of:

generating validity information for a packet, wherein the validity information comprises all necessary information required for performing a validity check of the packet;

generating a header for the packet, comprising the validity information;
and

sending the packet including the header from a first network node to a second network node.

2. The method according to claim 1, wherein the step of generating the validity information comprises generating security information indicating security services applied to the packet.

3. The method according to claim 1, wherein the step of generating the validity information comprises generating algorithm information to be used for performing the validity check of the packet.

4. The method according to claim 3, wherein the step of generating the algorithm information comprises generating the algorithm information which indicates an algorithm to be used for performing the validity check of the packet.

5. The method according to claim 3, wherein the step of generating the algorithm information comprises generating the algorithm information which comprises values to initialize an algorithm to be used for performing the validity check of the packet.

6. The method according to claim 1, wherein the step of generating the validity information comprises generating public key information of a sending node.

7. The method according to claim 6, wherein the step of generating the public key information comprises generating reference information related to how a public key can be obtained.

8. The method according to claim 7, wherein the step of generating the reference information comprises generating an identity of an entity from which the public key can be obtained.

9. The method according to claim 7, wherein the step of generating the reference information comprises generating a public key identifier for the public key.

10. The method according to claim 6, wherein the step of generating the public key information comprises generating the public key.

11. The method according to claim 6, wherein the step of generating the public key information comprises generating public key verification information indicating information in order to verify that the public key actually belongs to the sending node.

12. The method according to claim 1, wherein the step of generating the validity information comprises generating an information item for preventing replay attacks.

13. The method according to claim 12, wherein the step of generating the information item comprises including in the information item an indication of a procedure to be used for anti replay attacks.

14. The method according to claim 12, wherein the step of generating the information item comprises including in the information item a time stamp.

15. The method according to claim 6, further comprising the step of:
signing the packet using a private key corresponding to the Public Key indicated by the validity information in the packet header in a sending network node.

16. The method according to claim 1, further comprising the step of:
performing a validity check of the packet by referring to the validity information contained in the header of the packet in a receiving node.

17. The method according to claim 1, further comprising the step of:
performing a validity check of a packet by referring to the validity information contained in the header of the packet in an intermediate node.

18. A network node for sending packets to a receiving network node, comprising:

first generating means for generating validity information for a packet;

second generating means for generating a header for the packet, comprising the validity information; and

sending means for sending the packet including the header to a receiving network node,

wherein the validity information comprises all necessary information required for performing a validity check of the packet.

19. A network node comprising:

receiving means for receiving packets from a sending network node;
and

performing means for performing a validity check of a packet by referring to validity information contained in a header of the packet,

wherein the validity information comprises all necessary information required for performing the validity check of the packet.

20. A network node comprising:

forwarding means for forwarding packets from a sending network node to a receiving network node; and

performing means for performing a validity check of a packet by referring to validity information contained in a header of the packet ,

wherein the validity information comprises all necessary information required for performing a validity check of the packet.

21. The network node according to claim 18, wherein the validity information comprises security information indicating security services applied to the packet.

22. The network node according to claim 18, wherein the validity information comprises algorithm information indicating an algorithm to be used for performing the validity check of the packet.

23. The network node according to claim 18, wherein the validity information comprises public key information of a sending node.

24. The network node according to claim 23, wherein the public key information comprises reference information related to how a public key can be obtained.

25. The network node according to claim 24, wherein the reference information comprises an identity of an entity from which the public key can be obtained.

26. The network node according to claim 24, wherein the reference information comprises a public key identifier for the public key.

27. The network node according to claim 23, wherein the public key information comprises a public key.

28. The network node according to claim 23, wherein the public key information comprises public key verification information indicating

information in order to verify that the public key actually belongs to the sending node.

29. The network node according to claim 18, wherein the validity information comprises an information item for preventing replay attacks.

30. The network node according to claim 29, wherein the information item for preventing replay attacks contains an indication of a procedure to be used for anti-replay attacks.

31. The network node according to claim 29, wherein the information item for preventing replay attacks contains a time stamp.

32. The network node according to claim 23, further comprising:
signing means for signing the packet using a private key corresponding to a Public Key indicated by the validity information in the packet header in the sending network node.

33. The network node according to claim 18, wherein the network node comprises a mobile network node.

34. A network system comprising:
a first network node configured to send a packet, wherein the first network node comprises first generating means for generating validity information for a packet, second generating means for generating a header for the packet, comprising the validity information; sending means for sending the packet including the header to a receiving network node, wherein the validity information comprises all necessary information required for performing a validity check of the packet; and

a second network node configured to receive the packet, wherein the second network node comprises performing means for performing a validity check of a packet by referring to validity information contained in a header of the packet, wherein the validity information comprises all necessary information required for performing the validity check of the packet.

35. The network system according to claim 34, further comprising:
at least one intermediate node for forwarding packets from a sending network node to a receiving network node, wherein the at least one intermediate node comprises performing means for performing a validity check of a packet by referring to the validity information contained in a header of the packet.

36. The network node according to claim 19, wherein the validity information comprises security information indicating security services applied to the packet.

37. The network node according to claim 20, wherein the validity information comprises security information indicating security services applied to the packet.

38. The network node according to claim 19, wherein the validity information comprises algorithm information indicating an algorithm to be used for performing the validity check of the packet.

39. The network node according to claim 20, wherein the validity information comprises algorithm information indicating an algorithm to be used for performing the validity check of the packet.

40. The network node according to claim 19, wherein the validity information comprises public key information of a sending node.

41. The network node according to claim 20, wherein the validity information comprises public key information of a sending node.